Experimental Study on Channel Reciprocity in Wireless Key Generation

Experimental Study on Channel Reciprocity in Wireless Key Generation

(Invited Paper)

Junqing Zhang*, Roger Woods*, Trung Q. Duong*, Alan Marshall§, Yuan Ding*
* ECIT, Queen's University Belfast
Belfast, BT3 9DT, UK
Email: {jzhang20, r.woods, trung.q.duong, yding03}@qub.ac.uk
§ Department of Electrical Engineering and Electronics, University of Liverpool
Liverpool, L69 3GJ, UK
Email: Alan.Marshall@liverpool.ac.uk

***Abstract*—Key generation from wireless channels is a promising alternative to public key cryptography for the establishment of cryptographic keys. It is the first paper to experimentally study the channel reciprocity principle of key generation, through investigating and quantifying channel measurements' cross-correlation relationship affected by noise and non-simultaneous measurements. Channel measurements, both received signal strength and channel state information, are collected from a real experimental platform using the wireless open access research platform (WARP) in a multipath office room. We found that in a slow fading channel (e.g., with a coherence time of about 50 ms), the channel cross-correlation is impacted greatly by noise but little by non-simultaneous measurements with a small sampling time difference (e.g., 0.06 ms). The resolution of the sampling time difference can be satisfied by wireless systems such as IEEE 802.11 to maintain an acceptable cross-correlation coefficient without affecting the bandwidth and communication efficiency.**

***Index Terms*—Physical layer security, key generation, channel reciprocity**

I. Introduction

Due to its broadcast nature, wireless communication is vulnerable and thus protected by cryptographic schemes. These schemes normally require keys securely shared before transmission, which is usually carried out by public key cryptography (PKC), e.g., Diffie-Hellman key exchange protocol [1]. PKC relies on computational hardness and requires a public key infrastructure, which makes it unsuitable for low cost and computation-restricted devices and ad hoc networks.

Key generation from the randomness of wireless fading channels is a promising alternative and has received extensive research attention [2], because this technique is information-theoretically secure, lightweight and does not require any help from other users. There have been key generation systems reported by exploiting the randomness from received signal strength (RSS) and channel state information (CSI), which are available in commercial and customized hardware devices. CSI-based key generation has been applied in IEEE 802.11 g/n systems [3]–[5], while RSS has been used for key generation in IEEE 802.11 systems [6], [7], IEEE 802.15.4 systems [8]–[10] and Bluetooth systems [11].

Channel reciprocity principle indicates that the statistical features at each end of a wireless link are the same, which is the basis of the key generation. In practice, most of the commercial wireless devices work in half-duplex mode. Therefore, the legitimate users, Alice and Bob, measure the channel at the same frequency alternately at different time instants, i.e., key generation usually works in a time-duplex division (TDD) system and slow fading channel. In addition, hardware noises are independent and cannot be avoided. Therefore, the received signals at each node are not ideally symmetric due to the non-simultaneous measurements and noises. After Alice and Bob gather enough data, they quantize their asymmetric channel measurements into binary values separately, which will not always match. The disagreement of the quantized bits can then be corrected by information reconciliation stage, e.g., by using error correcting code [12], after which Alice and Bob will get the same key.

The similarity of two signals can be quantified by cross-correlation coefficient between them. So far, attempts to improve cross-correlation of the measurements can be largely sorted into two categories: interpolation [8], [9] and filtering [3], [10], [13], [14]. Interpolation emulates that the channel were measured at the same time while a filter can be employed to suppress the high frequency components of the noise.

We have theoretically modelled and analyzed the effects of non-simultaneous measurements and noise on the cross-correlation of the measurements in [15], and found that noise has a more dominant impact in a slow fading channel. In this paper, we carried out an experimental study. We implemented a key generation system using a customized hardware platform, wireless open access research platform (WARP) [16] and carried out an experiment to collect the real measurements data, i.e., both RSS and CSI. We connected two boards to a common antenna using a power splitter so that signals can be received simultaneously by them but affected separately by independent hardware noise. This arrangement enables us to investigate the effect of noise without the impact of non-simultaneous sampling and to quantify their contribution to the signal cross-correlation. Results have revealed that when the sampling time difference is small (e.g., 0.06 ms), noise is the main factor that influences the cross-correlation relationship of the measurements in a slow fading channel

(e.g., with coherence time as about 50 ms), which matches our theoretical analysis in [15]. We also found the resolution of the sampling time difference can be satisfied by wireless systems such as IEEE 802.11 to maintain an acceptable cross-correlation coefficient without affecting the bandwidth and communication efficiency.

The rest of the paper is organized as follows. Section II introduces the channel model and Section III presents our measurement system and test scenario. The evaluation metrics are described in Section IV and the experiment results are given in Section V. Section VI concludes the paper.

II. Channel Model

An experimental scenario is set up where Bob and Eve are connected to a common antenna via a balanced power splitter, as shown in Fig. 1(a). Alice, located several meters away from them, sends signals every T_s ms and the signal received by the common antenna of Bob and Eve is divided through the power splitter and routed to Bob and Eve simultaneously at time t_B. After Bob successfully receives the signal, he returns a signal to Alice which is also divided but at time t_A. All the signals are transmitted with the same power. The received signals of Alice, Bob, and Eve can be given respectively as

$$y_A(t_A) = \sqrt{G_{1s}} h(t_A, \tau) * x(t_A) + n_A(t_A), \quad (1)$$

$$y_B(t_B) = \sqrt{G_{s1}} h(t_B, \tau) * x(t_B) + n_B(t_B), \quad (2)$$

$$y_E(t_B) = \sqrt{G_{s2}} h(t_B, \tau) * x(t_B) + n_E(t_B), \quad (3)$$

where $*$ denotes the convolution, $h(t, \tau)$ is the channel impulse response (CIR), $n_u(t)$ is user u's hardware noise, u represents A, B or E, and G_{ij} is the transmission coefficient between ports i and j of the power splitter. In this way, the signal is received by Bob and Eve simultaneously and later affected by hardware noise independently. Therefore, the effect of the non-simultaneous measurements and noise on the correlation relationship can be separately evaluated.

The received powers of the users can be written as

$$P_A(t_A) = G_{1s} P(t_A) + P_A^n(t_A), \quad (4)$$

$$P_B(t_B) = G_{s1} P(t_B) + P_B^n(t_B), \quad (5)$$

$$P_E(t_B) = G_{s2} P(t_B) + P_E^n(t_B), \quad (6)$$

where $P(t)$ is the power of the signal $h(t, \tau) * x(t)$ and $P_u^n(t)$ is the power of noise residing in user u. The received power is usually reported as RSS in network interface cards (NICs).

In orthogonal frequency-division multiplexing (OFDM) systems, CSI can be estimated by training symbols, which is given as

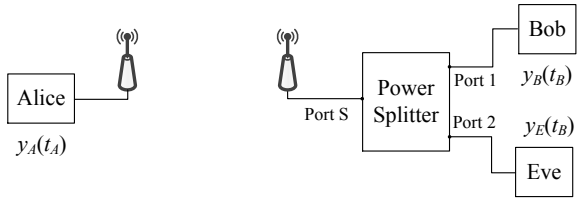
$$\widehat{H}_A(t_A, f_m) = \sqrt{G_{1s}} H(t_A, f_m) + \widehat{w}_A(t_A, f_m), \quad (7)$$

$$\widehat{H}_B(t_B, f_m) = \sqrt{G_{s1}} H(t_B, f_m) + \widehat{w}_B(t_B, f_m), \quad (8)$$

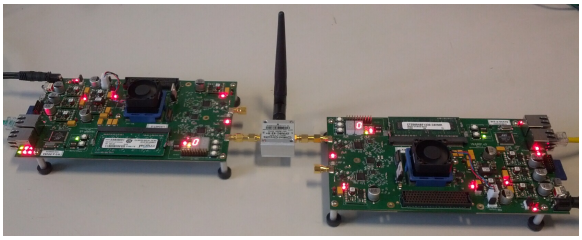
$$\widehat{H}_E(t_B, f_m) = \sqrt{G_{s2}} H(t_B, f_m) + \widehat{w}_E(t_B, f_m), \quad (9)$$

where $H(t, f_m)$ and $\widehat{w}_u(t, f_m)$ are the frequency domain counterparts of $h(t, \tau)$ and $n_u(t)$, respectively.

Both the received power and CSI contain channel randomness and can be exploited for key generation.



(a) Schematic diagram



(b) Bob and Eve connected to a common antenna via a power splitter

Fig. 1. Experiment setup

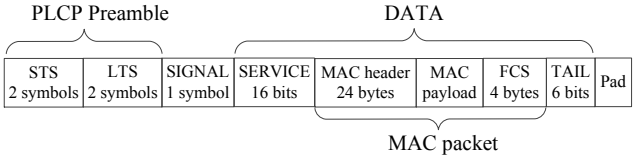


Fig. 2. Structure of IEEE 802.11 OFDM physical layer packet. The length of the blocks in the figure is not scaled.

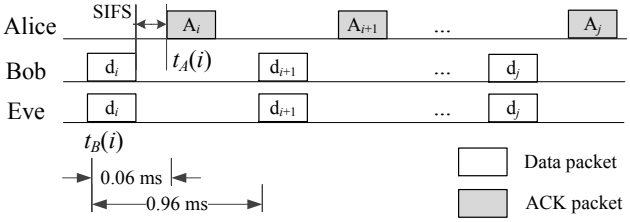


Fig. 3. Timing between ACK packets received by Alice and data packets received by Bob and Eve. The packet length and time intervals are not scaled.

III. Measurement System and Test Scenario

A measurement system is designed using WARP [16], a scalable and extensible wireless platform. The WARP 802.11 reference design is a real-time FPGA implementation of IEEE 802.11 distributed coordination function (DCF) MAC and OFDM physical (PHY) protocol. The physical packet structure is shown in Fig. 2. WARP boards and a PC are connected by a 1 Gbps Ethernet switch. The transmission information, such as timestamp, received power, and channel estimation, etc., can be stored in the PC for off-line processing.

According to the DCF MAC protocol, the receiver will send an ACKnowledgement (ACK) packet back to the transmitter upon the successful reception of the data packet after waiting a short interframe space (SIFS), as illustrated in Fig. 3. Both the data and ACK packet are modulated by OFDM, so the users can estimate the channel using the long training symbol (LTS)

in the preamble of the physical packet. The time difference between the data packet and corresponding ACK packet can be calculated as

$$\begin{aligned}\Delta t_{AB} &= t_{\text{data}} + t_{\text{SIFS}} \\ &= (5 + \lceil \frac{8l_{\text{data}} + 22}{N_{subc} N_{bpsc} R} \rceil) \frac{80}{B} + t_{\text{SIFS}}, \end{aligned} \tag{10}$$

where l_{data} is the byte number of MAC payload, N_{subc} is the number of data subcarriers, N_{bpsc} is the number of bits modulated to each subcarrier, R is the convolutional coding rate, B is the channel spacing, and t_{SIFS} is the time of the SIFS. In a $B = 20$ MHz channel spacing IEEE 802.11 system, $N_{subc} = 48$, $t_{\text{SIFS}} = 16$ μs, $R = \{1/2, 2/3, 3/4\}$, and $N_{bpsc} = \{1, 2, 4, 6\}$. The MAC fragmentation threshold is 2346 bytes [17], i.e., $28 \leq l_{\text{data}} \leq 2346$. The range of time difference can be calculated as

$$0.044 \text{ ms} \leq \Delta t_{AB} \leq 3.168 \text{ ms}. \tag{11}$$

As shown in Fig. 1(b), Bob and Eve were connected to the common antenna using a power splitter with a model of ZFRSC-42+ [18]. The power splitter can operate from DC to 4.2 GHz. It is specified in the manual that for 2.4 GHz operation, $G_{s1} = -6.03$ dB, $G_{s2} = -6.01$ dB and $G_{1s} = -5.95$ dB, whose values are almost the same. We also measured these transmission coefficients using a vector network analyzer, and the results are $G'_{s1} = G'_{s2} = G'_{1s} = -5.95$ dB, which match the specification.

All the users were running WARP 802.11 reference design and operating at $f_c = 2.412$ GHz center frequency. Alice and Bob were configured as an access point (AP) and a station (STA), respectively, while Eve was set as a passive listener. All the users were running at a data rate of 18 Mbps ($R = 3/4$, $N_{bpsc} = 2$) with a $l_{\text{data}} = 48$ bytes data payload. Under this configuration, $\Delta t_{AB} = 0.06$ ms. Alice was broadcasting Beacons every 100 ms to keep all the users synchronized. Alice was also sending data packets every $T_s = 0.96$ ms[1], whose power was divided by the power splitter evenly and received by Bob and Eve. The timing between the users' received packets is illustrated in Fig. 3.

The experiment was carried out in an office room with desks, chairs and cupboards, etc, which was considered to represent a typical multipath indoor environment. Alice was put on a trolley and moving at a speed of $v = 1$ m/s while Bob and Eve remained stationary. The experiment lasted 60 s and all the users recorded about 60,000 packets, which is enough for the numerical calculation of the correlation coefficient.

The channel was dynamic due to the movement of Alice. The coherence time is the time duration over which the channel stays unchanged and can be estimated as [19]

$$T_c = \frac{0.423}{f_d} = \frac{0.423c}{v f_c} = 52.6 \text{ ms}, \tag{12}$$

where f_d is the Doppler spread, c is the speed of light.

[1]The WARP 802.11 reference design requires a transmission resolution of 64 μs.

IV. Evaluation Metrics

The signal similarity can be quantified by the cross-correlation coefficient, which is defined as

$$\rho_{uv}^{X} = \frac{E\{X_u(t)X_v(t)\} - E\{X_u(t)\}E\{X_v(t)\}}{\sigma_{X_u}\sigma_{X_v}}, \tag{13}$$

where $E\{\cdot\}$ represents expectation operator, σ_X is the standard deviation of the signal X, and $X_u(t)$ denotes $P_u(t)$ or $|\widehat{H}_u(t, f_m)|$, $|\cdot|$ denotes the amplitude.

The channel measurements $X_u(t)$ can be quantized into binary values. Mean value-based quantization [7] is used as an example, which is given as

$$K_u^X(i) = \begin{cases} 1, & X_u(t_u(i)) > \mu_u; \quad (14a) \\ 0, & X_u(t_u(i)) \leq \mu_u, \quad (14b) \end{cases}$$

where $\mu_u = E\{X_u(t_u)\}$. Key disagreement rate (KDR) can then be calculated by comparing the keys generated by users, which is defined as

$$\mathit{KDR}_{uv}^{X} = \frac{\sum_{i=1}^{N} |K_u^X(i) - K_v^X(i)|}{N}. \tag{15}$$

The KDR is an essential parameter in key generation and determines the design of the information reconciliation stage.

It is noted that ρ_{AB}^X and KDR_{AB}^X are influenced by both non-simultaneous measurements and noise while ρ_{BE}^X and KDR_{BE}^X are only affected by noise because $X_B(t)$ and $X_E(t)$ have the same sampling time. Therefore, the effect of non-simultaneous measurements and noise can be separately analyzed.

The average correlation coefficient and KDR of CSI are calculated by averaging across all the subcarriers, given as

$$\bar{\rho}_{uv}^{|\widehat{H}|} = \frac{1}{M} \sum_{m=0}^{M-1} \rho_{uv}^{|\widehat{H}(f_m)|}, \tag{16}$$

and

$$\overline{\mathit{KDR}}_{uv}^{|\widehat{H}|} = \frac{1}{M} \sum_{m=0}^{M-1} \mathit{KDR}_{uv}^{|\widehat{H}(f_m)|}, \tag{17}$$

respectively, where M is the subcarrier's number of training symbols and $M = 52$ in IEEE 802.11 OFDM system.

V. Experiment Results

The received powers of Alice, Bob, and Eve in the first 10 s are shown in Fig. 4. The average absolute difference between these powers can be calculated as

$$\mu_{uv}^{|P|} = E\{|P_u(t) - P_v(t)|\}. \tag{18}$$

When the sampling time difference $\Delta t_{AB} = 0.06$ ms, $\mu_{AB}^{|P|} = 1.207$ dBm and $\mu_{BE}^{|P|} = 2.269$ dBm, which is quite small compared with the power variation and indicates a high consistence between each other. The correlation and KDR between the powers are calculated and shown in Fig. 5. It can be observed when $\Delta t_{AB} = 0.06$ ms, ρ_{AB}^P and ρ_{BE}^P are almost equal, and KDR_{AB}^P is very close to KDR_{BE}^P.

CSI of the first subcarrier of Alice, Bob and Eve in the first 10 s are shown as examples in Fig. 6. The correlation coefficients and KDRs between the subcarriers can be calculated

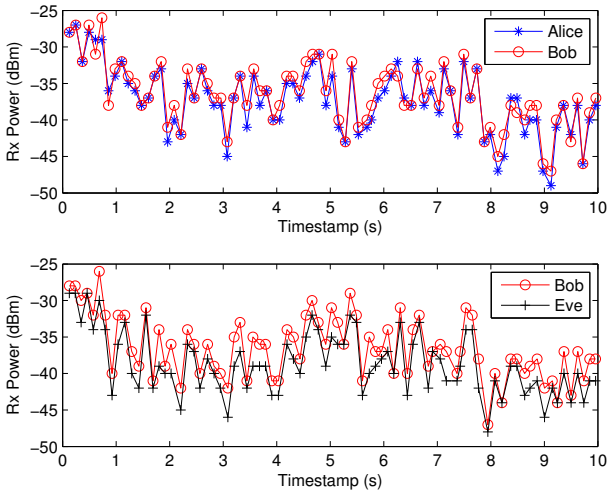


Fig. 4. Received powers of Alice, Bob and Eve, i.e., $P_A(t)$, $P_B(t)$, and $P_E(t)$. $\Delta t_{AB} = 0.06$ ms.

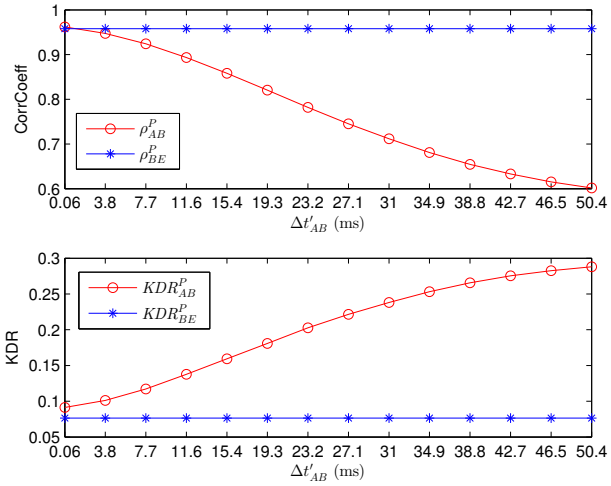


Fig. 5. ρ^P_{AB} and KDR^P_{AB} change versus $\Delta t'_{AB}$

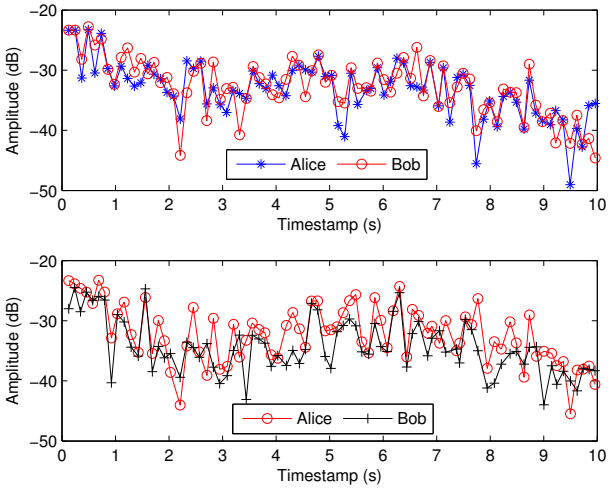


Fig. 6. Channel response of first subcarrier of Alice, Bob and Eve, i.e., $\widehat{H}_A(t, f_1)$, $\widehat{H}_B(t, f_1)$, and $\widehat{H}_E(t, f_1)$. $\Delta t_{AB} = 0.06$ ms.

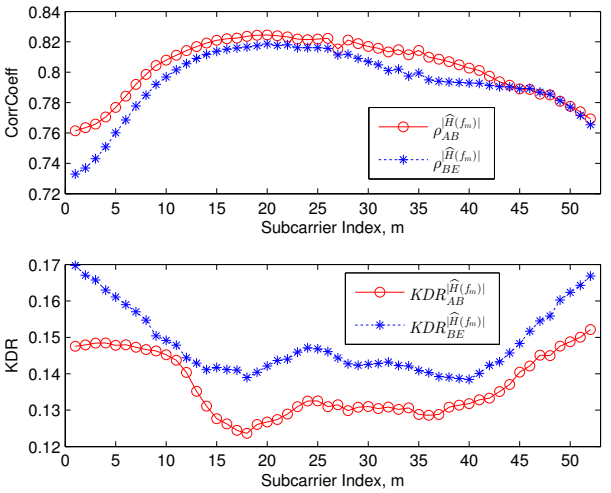


Fig. 7. Cross-correlation $\rho^{|\widehat{H}(f_m)|}_{AB}$ and KDR $KDR^{|\widehat{H}(f_m)|}_{AB}$ of all subcarriers. $\Delta t_{AB} = 0.06$ ms.

and shown in Fig. 7, which indicates that these correlation coefficients and KDRs match when $\Delta t_{AB} = 0.06$ ms.

Noise impacts on the cross-correlation and KDRs. As shown in Fig. 5 and Fig. 7, when Bob and Eve measure the channel simultaneously, $\rho^P_{BE} = 0.96$ and $\rho^{|\widehat{H}(f_m)|}_{BE}$ is around 0.8. It can also be observed that $\rho^P_{uv} > \rho^{|\widehat{H}(f_m)|}_{uv}$, i.e., noise is more detrimental to CSI. This is because received power is averaged over one packet and some of the noise effect is canceled out.

Further analyses are carried out by increasing the sampling time difference, which is achieved by changing the pairing between the records of data packets d_i at Bob and Eve and records of ACK packets A_j at Alice, as illustrated in Fig. 3. The time difference $\Delta t'_{AB}$ can be calculated as

$$\Delta t'_{AB} = 0.06 + (j - i) \times 0.96 \text{ ms}. \tag{19}$$

The correlation coefficients and KDRs of the received powers and CSI changes against sampling time difference $\Delta t'_{AB}$ are shown in Fig. 5 and Fig. 8, respectively. As can be observed from the figures, both ρ^P_{AB} and $\bar{\rho}^{|\widehat{H}|}_{AB}$ vary with $\Delta t'_{AB}$. In a slow fading channel such as Alice moving at a speed of 1 m/s and the coherence time is about 52.6 ms in this example, when increasing $\Delta t'_{AB}$ from 0.06 ms to 7.7 ms, ρ^P_{AB} drops from 0.96 to 0.92 while $\bar{\rho}^{|\widehat{H}|}_{AB}$ only decreases by less than 0.02; KDR^P_{AB} increases from 0.09 to 0.12 while $\overline{KDR}^{|\widehat{H}|}_{AB}$ only increases by less than 0.01. However, when $\Delta t'_{AB}$ is close to coherence time (i.e., 50.4 ms), ρ^P_{AB} and $\bar{\rho}^{|\widehat{H}|}_{AB}$ decrease by 0.36 and 0.17, respectively, which is quite significant. The acceptable $\Delta t'_{AB}$ is upper bounded as the key disagreement should be later corrected by information reconciliation. For example, a secure sketch scheme designed with BCH code $[n, k, t]$ can correct up to t/n disagreement [12], [14].

IEEE 802.11 OFDM systems use the LTS to estimate the

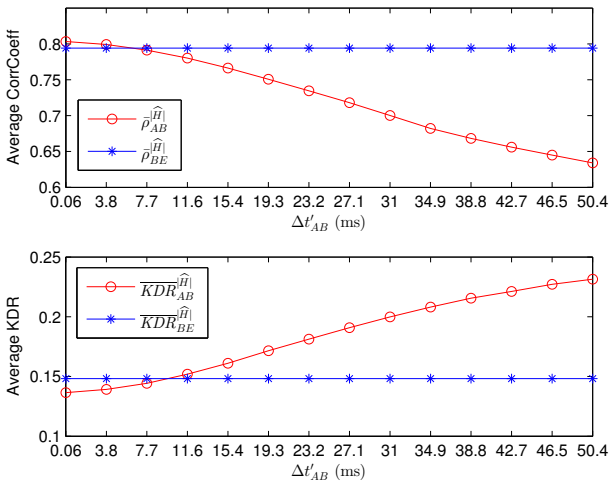


Fig. 8. $\bar{\rho}_{AB}^{|\widehat{H}|}$ and $\overline{KDR}_{AB}^{|\widehat{H}|}$ change versus $\Delta t'_{AB}$

channel and gets the received power by averaging over the entire packet, which is irrelevant of the content and length of the data payload. Even when the system reaches $\Delta t_{AB,\max} = 3.168$ ms with maximum data payload, ρ_{AB}^{P} and $\bar{\rho}_{AB}^{|\widehat{H}|}$ only decrease by less than 0.02 and 0.005, respectively, compared to the values measured at $\Delta t_{AB} = 0.06$ ms. This is beneficial as the key generation can be carried out by using routine data transmission rather than dedicated communication. The channel capacity and bandwidth of the communication system is not affected by the key generation.

VI. Conclusion

It is the first paper that experimentally studies the effect of non-simultaneous measurements and noise on the cross-correlation and KDR of the channel measurements in a slow fading channel. We implemented a testbed using WARP boards which are compatible with IEEE 802.11 DCF MAC and OFDM PHY protocol and can thereof provide both RSS and CSI. We connected two boards to a common antenna using a power splitter, allowing the received signals to be measured at the same time but affected by independent hardware noise separately. Through the analysis of cross-correlation coefficient and KDR calculated from the experiment data, we found that when the sampling time difference is small (e.g., 0.06 ms), channel correlation is more sensitive to noise in a slow fading channel (e.g., with coherence time as about 50 ms). We also found that the sampling time difference in routine communication can obtain an acceptable cross-correlation coefficient, which does not affect the bandwidth and communication efficiency. Our next step will be designing signal pre-processing algorithms to improve the cross-correlation relationship and decrease the KDR between the channel measurements at each keying node.

Acknowledgement

This work was supported by the Queen's University Belfast University Studentship, Newton Institutional Links Grant 172719890, Royal Academy of Engineering Research Fellowship under Grant RF1415\14\22, and US-Ireland R&D Partnership USI033 'WiPhyLoc8' grant involving Rice University (USA), University College Dublin (Ireland) and Queen's University Belfast (Northern Ireland). The authors also want to thank the WARP team for their continual help.

References

[1] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. 22, no. 6, pp. 644–654, 1976.
[2] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "Key generation from wireless channels: A review," *IEEE Access*, vol. 4, pp. 614–626, Mar. 2016.
[3] H. Liu, Y. Wang, J. Yang, and Y. Chen, "Fast and practical secret key extraction by exploiting channel response," in *Proc. 32nd IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Turin, Italy, Apr. 2013, pp. 3048–3056.
[4] W. Xi, X. Li, C. Qian, J. Han, S. Tang, J. Zhao, and K. Zhao, "KEEP: Fast secret key extraction protocol for D2D communication," in *Proc. 22nd IEEE Int. Symp. of Quality of Service (IWQoS)*, Hong Kong, May 2014, pp. 350–359.
[5] J. Zhang, R. Woods, A. Marshall, and T. Q. Duong, "Verification of key generation from individual OFDM subcarrier's channel response," in *Proc. IEEE GLOBECOM Workshop Trusted Commun. with Physical Layer Security (TCPLS)*, San Diego, California, USA, Dec. 2015, pp. 1–6.
[6] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: extracting a secret key from an unauthenticated wireless channel," in *Proc. 14th Annu. Int. Conf. Mobile Computing and Networking (MobiCom)*, San Francisco, California, USA, Sep. 2008, pp. 128–139.
[7] S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "On the effectiveness of secret key extraction from wireless signal strength in real environments," in *Proc. 15th Annu. Int. Conf. Mobile Computing and Networking (MobiCom)*, Beijing, China, Sep. 2009, pp. 321–332.
[8] N. Patwari, J. Croft, S. Jana, and S. K. Kasera, "High-rate uncorrelated bit extraction for shared secret key generation from channel measurements," *IEEE Trans. Mobile Comput.*, vol. 9, no. 1, pp. 17–30, Jan. 2010.
[9] H. Liu, J. Yang, Y. Wang, and Y. Chen, "Collaborative secret key extraction leveraging received signal strength in mobile wireless networks," in *Proc. 31st IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Orlando, Florida, USA, Mar. 2012, pp. 927–935.
[10] S. Ali, V. Sivaraman, and D. Ostry, "Eliminating reconciliation cost in secret key generation for body-worn health monitoring devices," *IEEE Trans. Mobile Comput.*, vol. 13, no. 12, pp. 2763–2776, Dec. 2014.
[11] S. N. Premnath, P. L. Gowda, S. K. Kasera, N. Patwari, and R. Ricci, "Secret key extraction using Bluetooth wireless signal strength measurements," in *Proc. 11th Annual IEEE Int. Conf. Sensing, Communication, and Networking (SECON)*, Singapore, Jun. 2014, pp. 293–301.
[12] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," *SIAM J. Comput.*, vol. 38, no. 1, pp. 97–139, 2008.
[13] X. Zhu, F. Xu, E. Novak, C. C. Tan, Q. Li, and G. Chen, "Extracting secret key from wireless link dynamics in vehicular environments," in *Proc. 32nd IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Turin, Italy, Apr. 2013, pp. 2283–2291.
[14] J. Zhang, R. Woods, A. Marshall, and T. Q. Duong, "An effective key generation system using improved channel reciprocity," in *Proc. IEEE Int. Conf. on Acoustics, Speech and Signal Processing (ICASSP)*, Brisbane, Australia, Apr. 2015, pp. 1727–1731.
[15] J. Zhang, A. Marshall, R. Woods, and T. Q. Duong, "Efficient key generation by exploiting randomness from channel responses of individual OFDM subcarriers," *IEEE Trans. Commun.*, vol. PP, no. 99, pp. 1–1, 2016.
[16] WARP Project. [Online]. Available: http://warpproject.org
[17] *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification*, IEEE Std. 802.11, 2012.
[18] Power Splitter/Combiner, ZFRSC-42+. [Online]. Available: http://194.75.38.69/pdfs/ZFRSC-42+.pdf
[19] T. S. Rappaport, *Wireless Communications: Principles and Practice*, 2nd ed. Prentice Hall, 2001.